

Audit Report



YEAR 2000 COMPLIANCE OF SELECTED
MISSION CRITICAL COMMAND, CONTROL,
AND COMMUNICATIONS SYSTEMS MANAGED BY
THE DEFENSE INFORMATION SYSTEMS AGENCY

Report No. 99-202

July 2, 1999

Office of the Inspector General
Department of Defense

OTIC QUALITY INSPECTED 2

19990805 108

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

AQI 99-11-1957

Additional Copies

To obtain additional copies of this audit report, contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or FAX (703) 604-8932 or visit the Inspector General, DoD Home Page at: www.dodig.osd.mil.

Suggestions for Audits

To suggest ideas for or to request future audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or FAX (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil, or by writing to the Defense Hotline, The Pentagon, Washington, DC 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

DISA	Defense Information Systems Agency
DITCO	Defense Information Technology Contracting Organization
FAR	Federal Acquisition Regulations
IT	Information Technology
Y2K	Year 2000



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-2884

July 2, 1999

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND,
CONTROL, COMMUNICATIONS, AND
INTELLIGENCE)
DIRECTOR, DEFENSE INFORMATION SYSTEMS
AGENCY

SUBJECT: Audit Report on Year 2000 Compliance of Selected Mission Critical
Command, Control, and Communications Systems Managed by the Defense
Information Systems Agency (Report No. 99-202)

We are providing this audit report for information and use. We considered management comments on a draft of this report in preparing the final report.

Comments on the draft of this report conformed to the requirements of DoD Directive 7650.3 and left no unresolved issues. Therefore, no additional comments are required.

We appreciate the courtesies extended to the audit staff. Questions on the audit should be directed to Mr. Garold E. Stephenson at (703) 604-9332 (DSN 664-9332) (gstephenson@dodig.osd.mil) or Mr. Kent E. Shaw at (703) 604-9228 (DSN 664-9228) (kshaw@dodig.osd.mil). See Appendix D for the report distribution. The audit team members are listed inside the back cover.

A handwritten signature in black ink, reading "Robert J. Lieberman", is positioned above the typed name.

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 99-202
(Project No. 9CC-0089)

July 2, 1999

Year 2000 Compliance of Selected Mission Critical Command, Control, and Communications Systems Managed by the Defense Information Systems Agency

Executive Summary

Introduction. This is one in a series of reports being issued by the Inspector General, DoD, in accordance with an informal partnership with the Chief Information Officer, DoD, to monitor DoD efforts to address the year 2000 computing challenge. For a listing of audit projects addressing the issue, see the year 2000 webpage on the IGnet at <http://www.ignet.gov>.

Objective. The overall objective was to determine whether the Defense Information Systems Agency (DISA) has adequately planned for and managed year 2000 conversion risks to avoid undue disruption to selected mission critical command, control, and communications systems used in support of Unified Command operations. Specifically, we reviewed year 2000 conversion risk assessments, contingency plans for mission critical systems, and continuity of operations plans for systems managed by the DISA and identified by unified commanders as mission critical to their operations.

Results. We reviewed 34 DISA mission critical systems. Of the 34 systems reviewed, as of May 17, 1999, DISA had certified 23 as Y2K compliant, seven were in the development phase and had not been tested, and four had been terminated. The DISA had made substantial progress to ensure that its mission critical systems were Y2K compliant but still needed to prepare contingency plans for the Defense Satellite Communications System and the Defense Information Systems Network Deployed (Step) Switch Multiplexer Unit system. The absence of contingency plans for the systems could have adversely affected the ability to complete mission requirements should a Y2K problem materialize (see Finding section).

Summary of Recommendation. We recommend that the Director, Defense Information Systems Agency prepare contingency plans for the Defense Satellite Communications System and the Defense Information Systems Network Deployed (Step) Switch Multiplexer Unit System.

Management Comments. We provided a draft of this report on May 17, 1999. Comments were received from the Y2K Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence), and the Inspector General, DISA. Both the Assistant Secretary of Defense and DISA concurred with the recommendation. The DISA stated that contingency plans for both the Defense Satellite Communications System and the Defense Information Systems Network Deployed (Step) Switch Multiplexer Unit System were being prepared and would be completed by June 20, 1999.

Table of Contents

Executive Summary	i
Introduction	
Background	1
Objective	3
Finding	
Y2K Compliance for DISA Mission Critical Systems	4
Appendixes	
A. Audit Process	7
Scope	7
Methodology	7
Summary of Prior Audits	8
B. Y2K Status of Mission Critical Systems	9
C. Report Distribution	12
Management Comments	
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)	14
Defense Information Systems Agency	15

Background

Problem Description. The year 2000 (Y2K) problem is the term most often used to describe the potential failure of information technology (IT) systems to process or perform date-related functions before, on, or after the turn of the century. The Y2K problem is rooted in the way that automated information systems record and compute dates. For the past several decades, systems have typically used two digits to represent the year, such as 98 representing 1998, to conserve on electronic data storage and reduce operating costs. However, the year 2000 is indistinguishable from the year 1900 with the two-digit format. As a result of the ambiguity, computers and associated system and application programs that use dates to calculate, compare, or sort could generate incorrect results when working with years following 1999. Calculation of Y2K dates is further complicated because the year 2000 is a leap year, the first century leap year since 1600. The computer systems and applications must recognize February 29, 2000, as a valid date.

DoD Y2K Management Plan. As the DoD, Chief Information Officer, the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) issued the "DoD Year 2000 Management Plan" (DoD Management Plan) in April 1997 and the most current version is dated December 1998. The DoD Management Plan provides the overall DoD strategy and guidance for inventorying, prioritizing, fixing, or retiring systems, and for monitoring progress. The DoD Chief Information Officer has overall responsibility for overseeing the DoD solution to the Y2K problem. The DoD Components are responsible for implementing the five-phase Y2K management process described in the DoD Management Plan. The DoD goals have been to complete implementation of Y2K compliant mission critical systems by December 31, 1998, and other systems by March 31, 1999.

Defense Information Systems Agency. The Defense Information Systems Agency (DISA) is the DoD agency responsible for information technology and is the central manager for major portions of the DoD information infrastructure. As a result, DISA is obligated to provide Y2K-compliant computing platforms, networks, and services to the DoD components.

Federal Acquisition Requirements. Federal Acquisition Regulation (FAR), subsection 39.106, "Year 2000 Compliance," requires agencies to ensure that solicitations and contracts pertaining to information technology acquisition be year 2000 compliant or require that noncompliant information technology be upgraded to year 2000 compliance prior to:

- Earliest date the information technology is required to perform date and time processing involving dates later than December 31, 1999, or
- December 31, 1999.

In addition, FAR, subsection 39.106, requires a description of existing information technology that will be used in conjunction with the information technology to acquire and identify whether the existing information technology is year 2000 compliant. Additionally, the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), in a memorandum, "Acquisition of Year 2000 (Y2K) Compliant Information Technology (IT) and Bringing Existing IT into Compliance," December 18, 1997, directed that orders for IT should not be placed against a contract or other acquisition instruments unless that contract or instrument requires Y2K compliance.

DISA Status Reporting. DISA tracks the Y2K completion status of mission critical systems and reports the status of each system in the Y2K process to Assistant Secretary of Defense Command, Control and Communications. The information that is maintained and reported on those systems includes status on: the Y2K phase, contingency plans, interface agreements, inclusion of references on FAR 39.106, and Y2K certification dates.

Certification Status System. The Deputy Secretary of Defense memorandum, "Year 2000 Verification of National Security Capabilities," August 24, 1998, requires that Defense agencies to certify they have tested the information technology and national security system in accordance with the Y2K Management Plan. In addition, each system certification must cite all mission-critical systems that are yet to be validated as Y2K compliant along with a timeline listing a deadline for validations.

DISA responded November 3, 1998, by providing certification status of mission critical systems and subsystems. The certification status included the following categories.

- Certified and validated systems that were Y2K compliant by December 31, 1998.
- Mission critical systems that will be certified and validated after December 31, 1998.
- Systems in the development stage representing new capabilities that would not be implemented before December 31, 1998.

Objective

The overall objective was to determine whether DISA had adequately planned for and managed year 2000 conversion risks to avoid undue disruption to selected mission critical command, control, and communications systems used in support of Unified Command operations. Specifically, we reviewed year 2000 conversion risk assessments, contingency plans for mission critical systems, and continuity of operations plans for systems managed by the DISA and identified by unified commanders as mission critical to their operations.

Y2K Compliance for DISA Mission Critical Systems

The DISA had made substantial progress to ensure that the mission critical systems were Y2K compliant in accordance with the DoD Year 2000 Management Plan. For the 34 mission critical systems reviewed, as of May 17, 1999, DISA had certified 23 as Y2K compliant, seven were still in the development phase and had not been tested, and four had been terminated. All of the systems that were reviewed had interface agreements where required, and incorporated the Y2K references in contracts for commercial hardware and software. However, two systems did not have the required contingency plans because the project managers had not insisted on approved contingency plans from the U.S. Army Communications and Electronics Command for both systems. The absence of contingency plans for the systems could have adversely affected the ability to complete mission requirements should a Y2K problem materialize.

Compliance with DoD Year 2000 Management Plan

The DoD Y2K Management Plan provides the guidelines to ensure that date-related processing of mission critical systems perform correctly before, on, and after January 1, 2000. The plan requires that the program manager of each mission critical system ensure that:

- systems are certified Y2K compliant unless officially retired,
- Y2K compliant language is in all new contracts and contract modifications,
- interface agreements or equivalent are documented and obtained for each system interface, and
- system contingency plans are developed and maintained.

Y2K Certification. The system developer and functional proponents are required to certify and document each system's Y2K compliance. Of the 34 mission critical systems reviewed, DISA had officially certified 23 as Y2K compliant in accordance with the DoD Y2K Management Plan, properly completed Y2K compliance checklists, and provided Y2K testing information and results. Seven systems were still in the development phase and had not been tested. These developmental systems either provide a new capability or will be replacing a Y2K compliant system, and therefore DISA had not placed as high a priority on testing them as on existing systems needing remediation.

Inclusion of Compliance Clause in Contracts. The DoD management plan requires that DoD purchase only Y2K compliant products. Contracts should be written to include the requirements found in FAR, part 39. New contracts written after August 1997 must reference the FAR and authorize purchases of Y2K compliant items only. Modifications of existing contracts requiring Y2K compliance for information technology and date chips are required before contracts can be used to procure information technology.

DISA has implemented the Y2K language of FAR, part 39 into its new and existing contracts, through its contracting organization, the Defense Information Technology Contracting Organization (DITCO). Since December 1997, DITCO has incorporated a Y2K compliance specification requirement in all new solicitations and contracts. For existing information technology contracts awarded prior to December 1997, DITCO incorporated the Y2K specifications into the contracts on a bilateral, no cost basis.

Interface Agreements. The DoD management plan also requires identification of systems data exchange interfaces and documentation of agreements between systems owners regarding data exchange formats and protocols. Data trading partners must agree on formats and schedules to ensure errors are not passed from one organization to another. All of the systems reviewed either had interface agreements or were covered by other agreements. The latter category includes communications transport systems with telecommunications electrical interfaces, which must comply with international and national standards such as the American National Standard Institute.

Contingency Plans. The DoD management plan strongly emphasizes that DoD Components develop realistic contingency plans for protection against system failure. The contingency plans provides insurance against the many types of Y2K disruptions by ensuring that plans are in place to restore the systems and to continue the mission or function while a system is not available. DISA had made progress to complete contingency plans for its mission critical systems. Twenty of the 34 systems reviewed had contingency plans. Of the 14 systems without contingency plans, ten were either terminated, being replaced, or in the development phase. Two systems were actually infrastructures for building systems. A contingency plan is needed for the system using the infrastructure. The remaining two systems, the Defense Satellite Communications System and the Defense Information Systems Network Deployed (Step) Switch Multiplexer Unit system, lacked required contingency plans. DISA senior managers agreed that both systems needed contingency plans, but believed that the U.S. Army Communications and Electronics Command should prepare and approve them.

Conclusion

The DISA had made substantial progress to ensure that the mission critical systems reviewed were Y2K compliant but still needs to prepare contingency

plans for the Defense Satellite Communications System and the Defense Information Systems Network Deployed (Step) Switch Multiplexer Unit system. The absence of contingency plans for these systems could adversely affect the ability to complete mission requirements should a Y2K problem materialize

Recommendation and Management Comments

We recommend that the Director, Defense Information Systems Agency develop contingency plans for the Defense Satellite Communications System and the Defense Information Systems Network Deployed (Step) Switch Multiplexer Unit System.

Management Comments. Both the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence), and the Inspector General, DISA concurred with the recommendation. The DISA IG stated that contingency plans for both the Defense Satellite Communications System and the Defense Information Systems Network Deployed (Step) Switch Multiplexer Unit System were being prepared and would be completed by June 20, 1999. The Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) concurred with DISA's comments. The full text of the responses is included in the Management Comments section of this report.

Appendix A. Audit Process

This is one in a series of reports being issued by the Inspector General, DoD, in accordance with an informal partnership with the Chief Information Officer, DoD, to monitor DoD efforts to address the Y2K computing challenge. For a listing of audit projects addressing the issue, see the Y2K web page on the IGnet at <http://www.ignet.gov>.

Scope

Audit Work Performed. We reviewed selected DISA mission critical systems for Y2K compliance. We met with DISA's Chief Information Officers, Program Managers, and other designated points of contact at DISA Headquarters, Arlington, VA, and its offices in Sterling, VA; Falls Church, VA; Reston, VA; and Annapolis, MD. For each system, we reviewed the.

- Certification checklist;
- interface agreements;
- contingency plans;
- contract provisions that incorporated Y2K language in FAR, subpart 39.106;
- selected systems deployment schedule; and
- DISA systems status reports.

As we reviewed these documents, we determined whether the systems had the required documentation required by the DoD Y2K management plan requirements.

Methodology

Audit Type, Dates, and Standards. We performed this program audit from January 1999 to April 1999, in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD. We did not use computer-processed data to perform this audit.

Contacts During the Audit. We visited or contacted individuals and organizations within DoD. Further details are available upon request.

Use of Technical Assistance and Computer Processed Data. We did not use technical assistance or computer-processed data to perform this audit.

Management Control Program. We did not review the management control program related to the overall audit objective because DoD recognized the Y2K issue as material management control weakness area in FY 1997 Annual Statement of Assurance.

DoD-Wide Corporate Level Government Performance and Results Act Goals. In response to the Government Performance Results Act, the Department of Defense has established six DoD-wide corporate-level performance objectives and 14 goals for meeting the objectives. This report pertains to achievement of the following objectives and goals.

- **Objective:** Prepare now for an uncertain future.
Goal: Pursue a focused modernization effort that maintains U.S. qualitative superiority in key war fighting capabilities (DoD-3)

DoD Functional Area Reform Goals. Most major DoD functional areas have also established performance improvement reform objectives and goals. This report pertains to achievement of the following objectives and goals.

- **Objective:** Become a mission partner.
Goal: Serve mission information users as customers. (ITM-1.2)
- **Objective:** Provide services that satisfy customer information needs.
Goal: Modernize and integrate DoD information infrastructure. (ITM-2.2)
- **Objective:** Provide services that satisfy customer information needs.
Goal: Upgrade technology base. (ITM-2.3)

General Accounting Office High-Risk Area. The General Accounting Office has specifically designated risk in resolution of the Y2K problem as high. This report provides coverage of that problem and of the overall Information Management and Technology high-risk area.

Summary of Prior Audits

The General Accounting Office and the Inspector General, DoD, have conducted multiple reviews related to Y2K issues. General Accounting Office reports can be accessed over the Internet at <http://www.gao.gov>. Inspector General, DoD, reports can be accessed over the Internet at <http://www.dodig.osd.mil>.

Appendix B. Y2K Status of Mission Critical Systems

<u>Systems under development:</u>	<u>Certified Year 2000 Compliant</u>	<u>Year 2000 Compliance Phase</u>	<u>Completed Year 2000 Testing</u>	<u>Documented Contingency Plans</u>	<u>Year 2000 FAR Clause 39.106</u>	<u>Completed Interface Agreements</u>
1. DISN Video Services Global	No	Development	No	Not Applicable (N/A)	Yes	Yes
2. DISN Enhanced Mobile Satellite System	No	Development	No	No	Yes	No
3. DISN Information Dissemination Management	No	Development	No	No	Yes	No
4. Global Combat Support System ¹	Yes	Development	Yes	N/A	N/A	Yes
5. Integrated Imagery Intelligence Database	No	Development	No	No	Yes	Yes
6. Spectrum XXI	No	Development	No	Yes	Yes	Yes
7. Theater Level Analysis Replanning and Graphical Environment	No	Development	No	No	Yes	No
 <u>Systems to be terminated prior to the year 2000:</u>						
1. Defense Integration Support Tools	N/A	Terminated	N/A	N/A	N/A	N/A
2. Management of Network Income Expense and Services	N/A	Terminated	N/A	N/A	N/A	N/A
3. Automated Resources Management System	N/A	Replaced	N/A	N/A	N/A	N/A
4. Joint Operations Planning and Execution System	N/A	Retirement	N/A	N/A	N/A	N/A

¹ A prototype of the Global Combat Support System was tested as Y2K compliant but the system as a whole is still under development. Once operational, the system will need to undergo system testing.

<u>Legacy systems that will continue to be used after the year 2000:</u>	<u>Certified Year 2000 Compliant</u>	<u>Year 2000 Compliance Phase</u>	<u>Completed Year 2000 Testing</u>	<u>Documented Contingency Plans</u>	<u>Year 2000 FAR Clause 39.106</u>	<u>Completed Interface Agreements</u>
1. Antidrug Network	Yes	Implementation	Yes	Yes	Yes	Yes
2. Automatic Digital Network	No	Completed	Yes	Yes	Yes	N/A
3. Common Operational Picture	Yes	Completed	Yes	N/A	Yes	N/A
4. DISN Asynchronous Transfer Mode	Yes	Completed	Yes	Yes	N/A	N/A
5. Defense Information Infrastructure Operating Environment	Yes	Completed	Yes	N/A	Yes	N/A
6. Defense Satellite Communications System (DSCS):	Yes	Completed	Yes	No	Yes	Yes
Network Planning Software ²	Yes	Completed	Yes	N/A	Yes	N/A
DSCS Automatic Spectrum Analyzer	Yes	Completed	Yes	N/A	Yes	N/A
DSCS Space	Yes	Completed	Yes	N/A	Yes	N/A
Production Satellite Comm Control Element	Yes	Completed	Yes	N/A	Yes	Yes
USC 28 Modem	Yes	Completed	Yes	N/A	Yes	Yes
7. Defense Information Systems Network Integrated	Yes	Completed	Yes	Yes	N/A	N/A
8. DISN Deployed (Step) Switch Multiplexer Unit	Yes	Completed	Yes	No	Yes	Yes
9. Defense Message System	Yes	Completed	Yes	Yes	Yes	Yes
10. Defense Red Switched Network	Yes	Implementation	Yes	Yes	Yes	N/A
11. Defense Switched Network ³	Yes	Implementation	Yes	Yes	Yes	N/A

² Although testing is complete on the Network Planning Software subsystem, DISA expects to replace the Network Planning Software subsystem with another system named the Common Network Planning Software.

³ DSN appears to be Y2K compliant; however, DISA has requested an independent audit of the test results for its American Telephone and Telegraph switch systems by the Joint Interoperability Test Command.

<u>Legacy systems that will continue to be used after the year 2000:</u>	<u>Certified Year 2000 Compliant</u>	<u>Year 2000 Compliance Phase</u>	<u>Completed Year 2000 Testing</u>	<u>Documented Contingency Plans</u>	<u>Year 2000 FAR Clause 39.106</u>	<u>Completed Interface Agreements</u>
12. Frequency Resource Records System Distributed Computing Facility	Yes	Completed	Yes	Yes	Yes	Yes
13. Frequency Resources Records System Central Computing Facility	Yes	Completed	Yes	Yes	Yes	Yes
14. Global Command and Control System (GCCS) (includes all components)	Yes ⁴	Completed	Yes	Yes	Yes	Yes
15. Integrated Digital Network Exchange	Yes	Completed	Yes	Yes	N/A	N/A
16. Integrated Network Management System	Yes	Completed	Yes	Yes	Yes	Yes
17. Joint Spectrum Management System	Yes	Completed	Yes	Yes	Yes	Yes
18. National C2 System Automated Message Handler	Yes	Completed	Yes	Yes	Yes	Yes
19. Sensitive Internet Protocol Router Network	Yes	Completed	Yes	Yes	N/A	N/A
20. Secret Internet Protocol Router Network	Yes	Completed	Yes	Yes	N/A	N/A
21. Terrain Integrated Rough Earth Model	Yes	Completed	Yes	Yes	Yes	N/A
22. Telecommunications Service Priority	Yes	Completed	Yes	Yes	Yes	N/A
23. World-Wide Online System Replacement	Yes	Completed	Yes	Yes	N/A	N/A

⁴ The DISA had certified the GCCS as Y2K compliant however the Inspector General, Department of Defense draft audit report "Status of Resources and Training System Year 2000 Issues," Project No 9LG-9019, April 16, 1999, has challenged the adequacy of that certification and testing procedures used for GCCS subsystems.

Appendix C. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition and Technology
Director, Defense Logistics Studies Information Exchange
Under Secretary of Defense (Comptroller)
Deputy Chief Financial Officer
Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
Deputy Assistant Secretary of Defense (Command, Control, Communications,
Intelligence, Reconnaissance, and Space Systems)
Deputy Chief Information Officer, and Deputy Assistant Secretary of Defense (Chief
Information Officer, Policy and Implementation)
Principal Director for Year 2000
Assistant Secretary of Defense (Public Affairs)

Joint Staff

Director, Joint Staff

Department of the Army

Assistant Secretary of the Army (Financial Management and Comptroller)
Inspector General, Department of the Army
Auditor General, Department of Army
Chief Information Officer, Army

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)
Inspector General, Department of the Navy
Auditor General, Department of the Navy
Inspector General, Marine Corps
Chief Information Officer, Navy
Superintendent, Naval Postgraduate School

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Inspector General, Department of the Air Force
Auditor General, Department of the Air Force
Chief Information Officer, Air Force

Defense Organizations

Director, Defense Contract Audit Agency
Director, Defense Information Systems Agency
 Inspector General, Defense Information Systems Agency
 Chief Information Officer, Defense Information Systems Agency
 United Kingdom Liaison Officer, Defense Systems Agency
Director, Defense Logistics Agency
Commandant, Defense Systems Management College
Inspector General, Defense Intelligence Agency
Inspector General, National Imagery and Mapping Agency
Inspector General, National Reconnaissance Office

Non-Defense Federal Organizations and Individuals

Office of Management and Budget
 Office of Information and Regulatory Affairs
General Accounting Office
 National Security and International Affairs Division
 Technical Information Center
 Director, Defense Information and Financial Management Systems, Accounting and
 Information Management Division, General Accounting Office

Congressional Committees and Subcommittees, Chairman, and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
Senate Special Committee on the Year 2000 Technology Problem
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Management, Information, and Technology,
 Committee on Government Reform
House Subcommittee on National Security, Veterans' Affairs, and International
 Relations, Committee on Government Reform
House Subcommittee on Technology, Committee on Science

Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Comments



Fax

Assistant Secretary of Defense
(Command, Control, Communications and Intelligence)
OASD C3I

DASD Y2K, Contingency Planning, Continuity
& Integration Management
(703) 602-0991 ext. 101
Fax: (703) 602-0994



INTERNET: Daniel.Green@osd.pentagon.mil

To: Mr. Kent E. Shaw (DODIG) From: Dan Green
Fax: (703) 604-9204 Pages: 1
Phone: Date: 06/14/99
Re: CC:

☐ Urgent ☐ For Review ☐ Please Comment ☐ Please Reply ☐ Please Recycle

Mr Shaw

Here is fax you requested. VR Dan Green

-----Original Message-----

From: Green, Daniel, CIV, OASD/C3I/Y2K
Sent: Friday, June 11, 1999 8:27 PM
To: Mr. Gerald E. Stephenson (DODIG); Mr. Kent E. Shaw (DODIG)
Subject: Concurrence of DODIG Audit Report on DISA Managed C3 Systems (Project No. 9CC-0089) (ASD(C3I) Control # 05-095/99)

Dear Mr. Stephenson, and Mr. Shaw,

The Y2K Contingency Planning Directorate in ASD(C3I) is in receipt of the following subject audit: "Audit Report of Audit of Y2K Compliance of Selected Mission Critical Command, Control, and Communications Systems Managed by DISA (Project No. 9CC-0089)."

With our review of your "draft" audit report we would like to provide you with the following concurrence. It is important for DISA to develop contingency plans for the DSCS and DISN Deployed (STEP) Switch Multiplexer Unit System. We believe that DISA's senior managers are correct in their assessment that "both systems need contingency plans".

I would like to state my appreciation for your efforts and to ask that you feel free to contact me at (703) 602-0991 ext 101, e-mail: Daniel.Green@osd.pentagon.mil if I can be of any further assistance.

VR
Dan Green
OASD(C3I)Y2K
Suite 920, Crystal Gateway 1
Daniel.Green@osd.pentagon.mil
(703) 602-0991 ext 101

PAGE 1

FAX:

JUN-14-99 MON 02:23 PM

Defense Information Systems Agency Comments



IN REPLY
REFER TO:

Inspector General (IG)

10 June 1999

DEFENSE INFORMATION SYSTEMS AGENCY

701 S. COURTHOUSE ROAD
ARLINGTON, VIRGINIA 22204-2199

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE
(ATTN: CONTRACT MANAGEMENT DIRECTORATE)

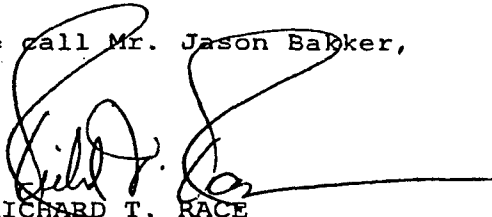
SUBJECT: Response to DoD IG Draft Report, Year 2000 Compliance
of Selected Mission Critical Command, Control, and
Communications Systems Managed by the Defense
Information Systems Agency (Project 9CC-0089)

1. The following is the Agency's response to the subject report:

Recommendation: ...DISA develop contingency plans for the
Defense Satellite Communications System and the Defense
Information Systems Network Deployed (STEP) Switch Multiplexer
Unit System.

Response: Both DSCS and DISN-D are non date processing and
thus category 5 systems, ones that require no management action
or system contingency plan. We are currently drafting a
system/operational contingency plan for both DSCS and DISN-D
(STEP), due June 20th. Both systems are certified Y2K compliant
and both are presently involved in higher level testing at the
Joint User Switch Exercises.

2. If you have any questions, please call Mr. Jason Bakker,
Audit Liaison, at (703) 607-6607.


RICHARD T. RACE
Inspector General

Quality Information for a Strong Defense

Audit Team Members

The Contract Management Directorate, Office of the Assistant Inspector General for Auditing, DoD, produced this report. Personnel of the Office of the Inspector General, DoD, who contributed to this report are listed below.

Garold E. Stephenson
Kent E. Shaw
Elaine M. Jennings
Steven I. Case
Robert E. Beets
George B. West, Jr.

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Year 2000 Compliance of Selected Mission Critical Command, Control, and Communications Systems Managed by The Defense Information Systems Agency

B. DATE Report Downloaded From the Internet: 08/05/99

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): **OAIG-AUD (ATTN: AFTS Audit Suggestions)**
 Inspector General, Department of Defense
 400 Army Navy Drive (Room 801)
 Arlington, VA 22202-2884

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ Preparation Date 08/05/99

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.